Math 148 Problem Set 1

April 19, 2025

1. HPS Problems: 1.41, 1.47, 2.7, 1.11 (Review theorem 1.11 which states the extended Euclidean algorithm).

2. Substitution Cipher: A disadvantage of the general substitution cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword `CIPHER` , write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

```
plain:   a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher:  C I P H E R A B D F G J K L M N O Q S T U V W X Y Z
```

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

```
C I P H E R
A B D F G J
K L M N O Q
S T U B W X
Y Z
```

This yields the sequence: `C A K S Y I B L T Z P D M U H F N V E G O W R J Q X`.

Such a system is used in the following decoded ciphertext:

```
FYRDMVYHSCDNBABBHSBHM
locationshavebeensent
MYYTZDFFVBSVJQDGZBADJOFVBN
toouralliesinzagrebandkiev
DLDVMVHGUTZMCBZKTBSMVYJS
awaitingfurtherquestions
```

Determine the keyword.

3. Big-$\mathcal{O}$ Notation: Label the following statements as true or false. For at least two of the statements, prove your claim using the definition of Big-$\mathcal{O}$.

1. $x^2 + \sqrt{x} = \mathcal{O}(x^2)$

2. $k^{2025} = \mathcal{O}(2^k)$
3. $2^k = \mathcal{O}(k^{2025})$
4. $e^{2k} = \mathcal{O}(k^2 2^k)$
5. $50\cos(r) + \sin(r) = \mathcal{O}(r)$

4. Binary Search: Suppose that Alice picks a number from 0 to y where $y \in \mathbb{N}$. Bob is trying to guess the number, and each time he makes an incorrect guess, Alice will tell him whether he is too high or too low. Design an algorithm that Bob can use to guess Alice's number that is better than brute force (guessing $1, 2, 3, \ldots$). Prove that your algorithm is better by calculating its time complexity as a function of of y, assuming that the only basic operation is the act of guessing a number.